ASA FAQ: Waarom stuurt de ASA pakketten naar de IPS module zonder IPS beleidsconfiguratie?

Inhoud

Inleiding

Dit document beschrijft waarom de Cisco adaptieve security applicatie (ASA) verkeer naar een ingesloten servicemodule voor inspectie zou kunnen doorsturen wanneer er geen IPS-modulebeleid (Inbraakpreventiesysteem) in de configuratie aanwezig is.

Q. Waarom stuurt de ASA pakketten naar de IPS module voor inspectie wanneer er geen IPS-beleid is ingesteld?

A.

Het is mogelijk dat een verbinding werd gebouwd om verkeer naar de IPS-module te sturen voor inspectie toen de ASA werd geconfigureerd, en dat verbinding nog actief is.

Zo heeft een klant met een ASA 5515-IPS geen geconfigureerd beleid in een beleidslijn om het verkeer naar de software IPS-module te sturen; het verkeer komt echter aan bij de module van de ASA.

Wanneer u de pakketweergavefunctie op IPS gebruikt, kunt u het verkeer zien dat naar IPS van de ASA komt:

```
14:34:38.341927 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.341992 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.345031 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
14:34:38.345068 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
```

De interfacestatistieken op de IPS-sensatieinterface werden gewist en er werden pakketten ontvangen:

```
sensor#  show interfaces portChannel
```

```
MAC statistics from interface PortChannel0/0
Interface function = Sensing interface
Description =
Media Type = backplane
Default Vlan = 0
InlineMode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Up
Admin Enabled Status = Enabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
Total Packets Received = 128
Total Bytes Received = 17904
Total Packets Transmitted = 128
Total Bytes Transmitted = 17904
```

De oorzaak van de kwestie is dat ergens in het verleden een configuratie werd toegevoegd aan de ASA om verkeer naar de IPS-module te sturen, en de verbindingen werden niet gewist nadat de IPS-configuratie was verwijderd op de ASA. Dit is gebruikelijk met niet-TCP protocollen die constant verkeer doorgeven.

Op de ASA, voer het **tonen** conn bevel in om te bepalen of de pakketten die u op de IPS module ziet verbindingsingangen hebben. Om de uptimes te zien, voer de opdracht **tonen in detail**. Om ervoor te zorgen dat de verbindingen niet opnieuw naar IPS worden gericht, kunt u het **heldere verbinding *<adres>***opdracht op de ASA moeten invoeren om deze specifieke verbindingen te wissen:

```
ASA# clear conn address 192.168.1.2
3 connection(s) deleted.
ASA#
```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems